REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-45 are presently active. Claims 1-45 have been presently amended.

In the outstanding Office Action, Claims 1-45 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cunningham et al (U.S. Pat. No. 6,321,337) in view of Reshef et al (U.S. Pat. No. 6,321,337).

Firstly, Applicants acknowledge with appreciation the courtesy of Examiner Parthasarathy to interview this case on July, 15, 2005 during which time the outstanding issues in the Office Action were discussed as summarized herebelow. During the interview, Applicants' representatives discussed the present invention in view of Applicants' Figure 1 and the description thereof in the specification. In particular, Dan Stevenson (who participated in the interview by telephone) explained how the intrusion-tolerant network, as defined in Claim 1, could for example be used by a web-based server such as Google to minimize the impact of an intrusion event (such as a Code Red Worm) on Google servers in which, due to the impact of the Code Red Worm, some of the Google servers would be suspect. As such individual ones of the Google servers would be directed to respond to a client request, producing "redundant" responses that under ideal conditions without the intrusion event would be the same response. However, with the occurrence of the intrusion event, not all servers may provide the same response (i.e., some of the responses may be corrupted).

In response to the intrusion event, the present invention as defined in Claim 1 can utilize an acceptance monitor and a ballot monitor to determine from the generated plural responses a preferred response to forward to the service requesting client. Processes such as the acceptance tests defined in Claim 10 and the balloting procedures defined in Claim 11 can be used to determine the proposed response.

While no agreement was reached during the interview, the features of a network acting on plural responses from protected servers and determining a preferred response to forward to the service-requesting client were viewed as features not previously searched for.

Accordingly, the present amendment clarifies the claimed intrusion-tolerant networks and claimed methods for reconfiguring communication among network components to more particularly point out the above-noted features. Applicants respectively submit that such features are not disclosed or suggested in the art of record.

For instance, Cunningham et al disclose a method and system for monitoring and controlling network access both inside and outside a network.[1] In Cunningham et al, there is a rule base distributed throughout the network to determine if a connection attempt should be completed or denied, or to decide if a previously established connection should be broken.[2] The Office Action acknowledges that Cunningham et al do not explicitly disclose receiving from an acceptance monitor the results of the applied acceptance tests and determining a preferred response to the client request. Moreover, the rule base in Cunningham et al, as shown in Figure 6, is applied functionally between the input port and the connection controller permitting firewall protection, as shown in Figures 1 and 2 of Cunningham et al. Thus, Cunningham et al disclose scrutiny of the incoming requests ***not scrutiny of the outgoing responses***, as in the claimed inventions.

The Office Action asserts that Reshef et al disclose a security gateway (proxy) positioned between external environment and a trusted server that controls access through acceptance rules wherein the security gateway receives from the access monitor the results of the applied acceptance tests and determines a preferred response to the client request.[3] However, the security gateway in Reshef et al is configured to protect the trusted server from

[1] Cunningham et al, see Abstract.
[2] Cunningham et al, see Abstract.
[3] Office Action, page 3, lines 17-22.

the external environment. As disclosed in Reshef et al, the security gateway converts external protocols into a simplified representation of the content to create a simplified message, thereby limiting the content which may be passed to the internal environment.[4] Like Cunningham et al, the purpose of Reshef et al is to protect the trusted server from the external environment (i.e., to protect the trusted server from incoming requests).

Thus, Cunningham et al with its firewall protection and Reshef et al with its security gateway both protect internal servers from disruptive incoming messages that may for example contain a worm or a virus. As such, neither Cunningham et al nor Reshef et al determine a preferred response from plural generated responses to forward to a service requesting client, as defined in the independent claims.

The significance of the distinction in information direction flow between Cunningham et al or Reshef et al and the present invention derives from the purposes of these respective systems. Whereas Cunningham et al and Reshef et al seek to protect servers from an external attack, at least one purpose of the present invention is to protect the integrity of an outgoing response to a service requesting client when the servers have been compromised. That is, when protective mechanisms like those provided by Cunningham et al and Reshef et al have failed.

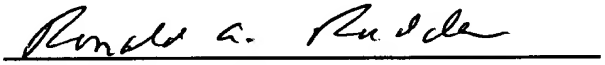
Thus, given these differences between Cunningham et al and Reshef et al, it is respectfully submitted that independent Claims 1, 2, 18, and 19 and the claims dependent therefrom patentably define over the applied prior art.

[4] Reshef et al, see Abstract.

Consequently, in view of the present amendment and in light of the above discussions, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Customer Number
22850

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
Ronald A. Rudder, Ph.D.
Registration No. 45,618

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/03)
GJM:RAR:clh
I:\ATTY\RAR\AMENDMENTS\271'S\271905US\AM1.DOC